

**FACTORS INFLUENCING ELECTRONIC FRAUD IN BANKING  
INDUSTRY IN TANZANIA: A CASE STUDY OF PEOPLES BANK OF  
ZANZIBAR**

**HAJI MAULID**

**A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT FOR THE  
REQUIREMENT OF THE DEGREE OF MASTER OF BUSINESS  
ADMINISTRATION OF THE OPEN UNIVERSITY OF TANZANIA**

**2019**

### CERTIFICATION

The undersigned certifies that he has read and hereby recommends for acceptance by the Open University of Tanzania a dissertation titled; "Factors Influencing Electronic Fraud in Banking Industry in Tanzania: A Case Study of Peoples Bank of Zanzibar" in partial fulfillment of the requirements for the degree of Master of Business Administration of the Open University of Tanzania.

.....

Dr. Salum Soud Mohamed

(Supervisor)

.....

Date

**COPYRIGHT**

No part of this dissertation may be reproduced, stored in any retrieval system, or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the author or the Open University of Tanzania in that behalf.

**DECLARATION**

I, Haji Maulid, do here declare that this dissertation is my own original work and that it has not been and will not be presented to any other University for similar or any other degree award.

í í í í í í í í í í í í í í

Signature

í í í í í í í í í í .í í í ..

Date

**DEDICATION**

I dedicate this dissertation to Almighty God who gave me life, idea, courage and power to pursue the study and my beloved parent Mr. Maulid Rajab and to my uncle Mr. Ramadhan Haji, their sacrifice through my education life cycle have been critical to my success.

## **ACKNOWLEDGEMENT**

I wish to convey my heartfelt thanks and appreciation to all those who, in one way or another, contributed to the successful completion of this dissertation. Particularly, special thanks should go to my supervisor, Dr. Salum Soud Mohamed for his guidance, support, monitoring and being involved with me in this study from the initial stage up to the end.

I would also thank my father Maulid Rajab for, among other things, their lifelong support in my academics throughout my career and my wife, Aisha Mahboob for her moral support and patience during the whole period of my course. My deepest and heartedly words of appreciation go to class mates, for being a strong supporter to me throughout my studies. I wish to thank Mr. Hamid Abdalla for providing me with their constructive inputs that have been very useful in completing this work.

Lastly, I acknowledge the contributions and supports of all who gave me constructive ideas and participation during the whole process, from the research proposal to the dissertation report production and to those who have helped me during the survey phase, data collection phase and data analysis phase, I thank them all. Errors or omissions are solely mine.

## ABSTRACT

The study was examined how banking industry in Tanzania protects customers through electronic banking services. E-banking is becoming more important in bank system because fraud affecting productivity of the banking services. The study realizes that due to some unfaithful persons, hackers and cybercriminals have taken advantage of the modality of concluding e-banking to deceive, or mislead any payment. Frauds in e-banking services globally occur as a result of various compromises in security ranging from weak authentication systems to insufficient internal controls. In this research the population of the study are all bank staff that is working inside People bank of Zanzibar limited in different branches in Tanzania. The purposive sampling technique was used to select the respondents. The author uses a sample of 30 banking experts to answer the questionnaires to represent the population. The banking officials chosen have a great knowledge of the technical issues related to the factors influencing electronic fraud in Tanzania. The study used majority of its respondents from fraud auditors and supervisors who had the primary responsibility of detecting and preventing fraud. The respondents accept strengthening of internal controls and systems was very effective strategy by 93.3%, improving numeration packages was effective by 100% but introducing hotlines and call centres was effective but not much. Other strategies were also seen effective including mandatory vacations and shuffling. The conclusion shows that People Bank of Zanzibar have good internal controls to combat fraud cases especially online frauds. PBZ gives it workers ethics trainings to stop them committing fraud. And lastly, the researcher concluded that PBZ staff is being paid good remunerations in order to prevent them of committing fraud cases.

## TABLE OF CONTENTS

<b>CERTIFICATION.....</b>	<b>ii</b>
<b>COPYRIGHT .....</b>	<b>iii</b>
<b>DECLARATION .....</b>	<b>iv</b>
<b>DEDICATION .....</b>	<b>v</b>
<b>ACKNOWLEDGEMENT.....</b>	<b>vi</b>
<b>ABSTRACT .....</b>	<b>vii</b>
<b>TABLE OF CONTENTS.....</b>	<b>viii</b>
<b>LIST OF TABLES.....</b>	<b>xiii</b>
<b>LIST OF FIGURE .....</b>	<b>xiv</b>
<b>LIST OF ABBREVIATIONS.....</b>	<b>xv</b>
<b>CHAPTER ONE .....</b>	<b>1</b>
<b>INTRODUCTION .....</b>	<b>1</b>
1.1 Background of the Study .....	1
1.2 Statement of the Research Problem .....	4
1.3 Objectives of the Study .....	6
1.3.1 General Objective.....	6
1.3.2 Specific Objectives.....	6
1.4 Research Questions .....	6
1.5 Significance of the Study.....	7
1.6 Scope of the Research .....	7
1.7 Organization of the Study.....	8



<b>CHAPTER TWO.....</b>	<b>9</b>
<b>LITERATURE REVIEW.....</b>	<b>9</b>
2.1 Introduction.....	9
2.2 Conceptual Definitions.....	9
2.2.1 Fraud.....	9
2.2.2 Control Systems .....	10
2.2.3 Factors .....	10
2.2.4 Electronic Banking.....	10
2.3 Theoretical Literature Review .....	10
2.3.1 Management Fraud.....	10
2.3.2 Employee Fraud .....	11
2.3.3 Third Party Fraud .....	12
2.3.4 Controlling Fraud mechanism .....	14
2.3.5 Fraud in International Countries .....	20
2.3.6 Bank Model .....	23
2.4 Empirical Literature Review.....	24
2.4.1 Empirical Literature Review Worldwide .....	24
2.4.2 Empirical Literature Review in Africa.....	27
2.4.3 Empirical Literature Review in Tanzania.....	31
2.5 Research Gap .....	33
2.6 Conceptual Framework .....	34
2.7 Theoretical Framework .....	34

<b>CHAPTER THREE .....</b>	<b>36</b>
<b>RESEARCH METHODOLOGY .....</b>	<b>36</b>
3.1 Introduction.....	36
3.2 Research Design.....	36
3.3 Area of the Study .....	37
3.4 Population of the Study .....	37
3.5 Sampling Design and Sample Size .....	38
3.5.1 Sampling Design.....	38
3.5.2 Sample Size .....	38
3.6 Data Collection Methods.....	39
3.7 Data Collection Tools.....	40
3.8 Reliability and Validity of Data.....	41
3.8.1 Data Reliability .....	41
3.8.2 Data Validity.....	41
3.9 Data Analysis.....	42
3.10 Ethical and Legal Issues .....	42
<b>CHAPTER FOUR .....</b>	<b>44</b>
<b>DATA ANALYSIS.....</b>	<b>44</b>
4.1 Introduction.....	44
4.2 Demographic Information .....	44
4.2.1 Gender .....	44
4.2.2 Age .....	45
4.2.3 Education Level .....	45
4.2.4 Role at Work.....	45

4.2.5	Experience .....	46
4.3	Perception of Fraud in PBZ Bank Limited.....	46
4.4	Management Fraud.....	48
4.5	Employee Fraud .....	48
4.6	Forms of Third-Party Fraud.....	49
4.7	Prevention and Control of Fraud.....	50
4.7.1	Strengthening of the Internal Control.....	50
4.7.2	Assessment and Prosecution of Fraud Cases.....	51
4.7.3	Higher Remuneration for Employees.....	51
4.7.4	Having Policies to Track Employees Conduct and Background.....	52
4.7.5	Establishing fraud Reporting Centres and Hotlines .....	52
4.7.6	Ensuring shuffling and Mandatory Vacations for Employees.....	53
4.7.7	Other Strategies.....	54
4.8	Discussion of the Findings .....	54
<b>CHAPTER FIVE .....</b>		<b>58</b>
<b>CONCLUSIONS &amp; RECOMMENDATIONS.....</b>		<b>58</b>
5.1	Introduction.....	58
5.2	Summary of the Main Findings .....	58
5.3	Implications of the Findings .....	60
5.4	Conclusion .....	61
5.5	Recommendations .....	61
5.5.1	Recommendations to the Bank .....	61
5.5.2	Recommendations to the Bank Regulator .....	62
5.6	Research Limitations.....	62

5.7	Recommendations for Further Studies .....	63
<b>REFERENCE</b>	.....	<b>65</b>
<b>APPENDIX</b>	.....	<b>72</b>

## LIST OF TABLES

Table 4.1: Demographic Information.....	44
Table 4.2: Perception of Fraud in PBZ bank Limited.....	47
Table 4.3: Management Fraud.....	48
Table 4.4: Employee Fraud .....	49
Table 4.5: Third Party Fraud .....	49
Table 4.6: Strengthening of Internal Control.....	50
Table 4.7: Assessment and Prosecution of Fraud Cases .....	51
Table 4.8: Higher Numeration of Employees.....	52
Table 4.9: Having Policies to Track employees Conduct .....	52
Table 4.10: Establishing Fraud Reporting Centers and Hotlines.....	53
Table 4.11: Ensuring shuffling and Mandatory Vacations for Employees .....	53

## LIST OF FIGURE

Figure 2.1: Conceptual Framework .....	34
--	----

**LIST OF ABBREVIATIONS**

CIMA	Chartered Institute of Management Accountants
Ltd	Limited
PwC	PricewaterhouseCoopers
PBZ	People Bank of Zanzibar
Shs	Shillings
SPSS	Statistical Product for Social Sciences
Tz	Tanzania

## **CHAPTER ONE**

### **INTRODUCTION**

#### **1.1 Background of the Study**

Electronic banking services are the banking class of services that can be offered by a bank to individuals and companies through electronic means via a fixed or mobile telephone, and Internet (RATI, 2011). Given that internet technology has evolved considerably over the years, newly developed e-banking services now differ considerably from older systems (Khan, 2009). Some of the more common types of E-Banking services today are Online Banking, Automated Teller Machines (ATM), Electronic Funds Transfer, Electronic Cheque Conversion, Direct Payment and Web ATM services (World Bank, 2018).

In the recent years, most financial institutions have adopted financial innovation in developing innovative products and offering wide range of services so as to increase efficiency and productivity which is the main objectives (Anyango 2015). Majority of customers in developing countries like Tanzania access their banking services and facilities using electronic mobile devices such as mobile phones. According to Saleem 2011, Tanzania has had dramatic changes in banking sector which has been made possible due to new technology. Electronic banking has been in a variety of platforms like online banking, telephone banking, TV-based banking, mobile phone banking, and offline banking.

Financial innovation through the use of Automated teller machines and deposit machines coupled with E-banking has enabled customers to carry out banking transactions without going to the banking hall. This encourages cash less society



where customers do not pay for their transaction using hard cash, but through electronic transfers of credit to their settlers' accounts (Aduda 2015). The online banking channel is the cheapest delivery channel for delivering banking products once established (Pikkarainen, 2004). Therefore, it is no surprise that the banks globally are continuing to shift towards e-banking services. With the growing support of e-banking services and its anticipated dominance in the near future, some of the known factors that contribute to addressing the critical problem of security must be addressed.

This paper identifies and synthesises a number of those factors such as the availability of funds, change management, timely access to information and strict internal controls could all prove vital for reducing e-banking fraud. Exposure to such factors provides regulators and bank management teams an insight into areas that may require increased emphasis and improvement. In the 21st century, modern technology and information technology have developed at an astonishingly swift pace. With the development of internet services as core, these modern technologies have been widely applied globally, especially in electronic banking services.

Since the first establishment of electronic banking in the United States on 18 October 1995, today's world has become an Internet-based world with information technology as a growing trend. World trade has been changed rapidly since the introduction of the internet and the World Wide Web, with electronic commerce transactions playing an important role in the current economy. According to Turban et al. (2003), electronic commerce has had a significant impact on the development of market and industrial culture. Not only does it alter products and services, it also

brings numerous changes to consumer behaviour and labour market. Local banks are among the victims of the largest global heist in which financial institutions lost an estimated \$1 billion after hackers--mainly from Eastern Europe, Ukraine, Russia and China--broke into the banks' network between 2013 and 2014.

The hackers targeted as many as 100 banks, e-payment systems and other financial institutions in 30 countries--including Tanzania, the US, China and European nations--and stole as much as \$10 million in each raid, according to a report released by Russia's largest maker of anti-virus software, (Kaspersky Lab, 2014). NBC Limited was among the local banks that were hit in the online raid. Hackers managed to withdraw hundreds of millions from Automated Teller Machines (ATMs) from within and outside Tanzania. Virtually all mainstream local banks have in recent weeks been victims of a huge number of ATM thefts that have cost the institutions billions of shillings and left customers in great distress.

The People's Bank of Zanzibar Limited (PBZ) is one among the oldest commercial banks in Tanzania. It is fully owned by the Government of Zanzibar. PBZ is the only bank in Tanzania with its head office in Zanzibar. It dominates the Zanzibar market with about 50% of the market share formed of the cosmopolitan population of over 1.0 million people. Zanzibar enjoys leading tourist investments from various countries. The bank does both retail and corporate banking with equipped modern systems that facilitate banking business locally and overseas efficiently. (PBZ 2012) The revolution of Information and Communications Technology has provided a base to banking industries to change their operations in betterment of their consumers from which efficiency and

competence are achieved with the adoption of several technologies (Ovia, 2005).

Since PBZ was established, it has only one branch located in Zanzibar with slight number of customers due to unsatisfied bank operations services. Currently PBZ is moving fast to expand its services in different factors by opening a branch in mainland and four branches the Island. Adoption of several technologies in PBZ Banking will allow consumers to be equipped with several options that will increase the industry efficiency in their daily banking procedures.

## **1.2 Statement of the Research Problem**

The role of the banking sector in strengthening the national economy is a primary reason that supports the current study on fraud monitoring and prevention in the Tanzanian banking sector environment. Any laxity in the national treasury poses a dangerous threat to the survival of the country socio-economic pursuits. Therefore, the present experience of fraud in the Tanzanian banking sector has the chance of increasing if not monitored and subsequently prevented.

In Tanzania fraud has been hitting in every bank so far, according to Ubwani (2016) on East-African newspaper said that almost 80 Million Tanzanian shillings was mysterious withdrawn from the account of Zanzibar-based East African Kiswahili Commission and later returned by yet to be identified people. EALA lawmakers have fingered KCB Zanzibar, where the account was held, for failing to cooperate in the investigations. EAC Secretariat told to act on the findings of the report and that those found culpable are punished ōso that there is no repeat of such thing in futureö. This is only one clear example that was documented but these issues have been

ongoing in different banks and fraud is increasing daily. While fraud has been identified as a major challenge and issue in most of private banks located in Tanzania which include PBZ and Barclays banks in the islands of Zanzibar (BOT,2013), very few scholars or studies have sought to establish the causes and strategies to combat fraud in the financial sector. This may have had a negative impact on policy making as policy solutions to fraud were not necessarily informed by empirical evidence.

Although some studies have been done in conjunction with Ministry of Finance and Planning of Tanzania and Bank of Tanzania (BOT), these studies are not available to local citizens and researchers as they are institutional properties. This has created a research and practice gap in the region as whole. This study sought to fill this gap by investigating the factors that contribute to electronic fraud in the banking industry in Tanzania. E-Banking fraud is an issue being experienced globally and is continuing to prove costly to both banks and customers. Frauds in e-banking services occur as a result of various compromises in security ranging from weak authentication systems to insufficient internal controls. Lack of research in this area is problematic for practitioners so there is need to conduct research to help improve security and prevent stakeholders from losing confidence in the system.

The purpose of this paper is to be aware of the factors that influence electronic fraud in banking industry in Tanzania, and continuing in the end to give the viable and realistic recommendations that is suitable to our banking sectors setup in Tanzania. Reported researches including (Adeyemi,2016) have concentrated on Factors Influencing Electronic Fraud in Banking Industry. However, there is a dilemma on

the factors that exactly influence electronic fraud in banking industry. This research intends to analyse factors Influencing E-Fraud in banking Industry in Tanzania with People Bank of Zanzibar (PBZ) which is a bank to most of customers as a case study.

### **1.3 Objectives of the Study**

#### **1.3.1 General Objective**

The general objective of this study was to analyse the factors influencing electronic fraud in banking industry in Tanzania with PBZ as a case study.

#### **1.3.2 Specific Objectives**

- i. To examine how management are aware of electronic fraud in PBZ bank.
- ii. To examine how the employees influencing electronic fraud in PBZ bank.
- iii. To examine how third-party activities influencing electronic fraud in PBZ bank.
- iv. To determine appropriate strategies to prevent and control E-fraud in PBZ bank.

### **1.4 Research Questions**

This research had ought to answer the following questions in order to improve performance and efficiency in our local banks in Tanzania and Zanzibar.

- i. To what level does the management are aware of electronic fraud in PBZ bank?
- ii. What are the factors that influence employees in committing electronic fraud in People Bank of Zanzibar Limited?

- iii. What are the third-party activities that leads to electronic fraud in PBZ bank?
- iv. What are the suitable preventions of the mentioned fraud concerns?

### **1.5 Significance of the Study**

The major deliverable was to highlight the factors which encourage electronic fraud to be used in the banking sector in Tanzania and the reasons why people are not aware of the problem so far, many factors either externally or internally was investigated in this research which result to E-Fraud in different transactions in the banks which starts from online usage to ATMs. The big significance of this project was to provide the empirical information and solutions to the banks including market professionals, shareholders of different banking institutions, without forgetting policy makers of the finance institutions inside the banks or in the governments of Tanzania,

This research will help them make better solutions in implementing the security systems or (E-fraud controlling methods) so that it can increase bank management commitment and profitability inside the banking systems. The findings of this study will surely elaborate the understandings and clarity of the customer's perceptions and expectations of the quality of banking services in Tanzania (Zanzibar town) since most of the customer's information were provided in chapter three of this research, and this will guide the banks to understand the customers better.

### **1.6 Scope of the Research**

The scope of the research was limited to Tanzania banking system and focus only on electronic fraud. The scope was limited to People bank of Zanzibar only which has

several branches in Tanzania, but the research concentrated to those branches which are found in Zanzibar.

### **1.7 Organization of the Study**

This research started with explanations of various contents with the inclusion of problem context, objectives and limitations of the study. Literature review will be seen in second chapter which includes the deep concepts of electronic fraud in banking industry in Tanzania, the methodology used to this research which includes research design with the research instrument will be demonstrated and shown in chapter three. Where as in chapter four it shows the result and analysis of the whole survey which includes the data analysis. And last chapter which is chapter five of this study is conclusion, implications and recommendation for the future usage of the study.

## **CHAPTER TWO**

### **LITERATURE REVIEW**

#### **2.1 Introduction**

The revolution of Information and Communications Technology has provided a base to banking industries to change their operations in betterment of their consumers from which efficiency and competence are achieved with the adoption of several technologies (Pan et al., 2011). The People's Bank of Zanzibar Limited (PBZ) is one among the oldest commercial banks in Tanzania. It is fully owned by the Government of Zanzibar. PBZ is the only bank in Tanzania with its head office in Zanzibar. It dominates the Zanzibar market with about 50% of the market share formed of the cosmopolitan population of over 1.4 million people. Zanzibar enjoys leading tourist investments from various countries. The Bank does both retail and corporate banking with equipped modern systems that facilitate banking business locally and overseas efficiently. (PBZ 2012)

Since PBZ was established, it has only one branch located in Zanzibar with slight number of customers due to unsatisfied bank operations services. Currently PBZ is moving fast to expand its services in different factors by opening a branch in mainland and four branches the Island. Adoption of several technologies in PBZ Banking will allow consumers to be equipped with several options that will increase the industry efficiency in their daily banking procedures.

#### **2.2 Conceptual Definitions**

##### **2.2.1 Fraud**

Fraud is a deliberate deception to obtain illicit material gain, and includes



embezzlement and asset misappropriation (Pan et al., 2011).

### **2.2.2 Control Systems**

A control system consists of subsystems and processes put together for the purpose of controlling the outputs of the process (Ganesh 2008).

### **2.2.3 Factors**

A constituent or element that brings about certain effects or results, or indicates a specific multiple, number, amount or quantity. (Dawson,2018).

### **2.2.4 Electronic Banking**

The use of computers to carry out banking transactions such as withdrawals through cash dispensers or transfer of funds at point of sale ( Pal,2016)

## **2.3 Theoretical Literature Review**

Fraud has been classified in various ways using various parameters: Management fraud, Insiders who are purely employees of the banks, outsiders who are customers or noncustomers of the banks and insiders /outsiders, which is a partnership of the employees (insiders) and outsiders.

### **2.3.1 Management Fraud**

This is frequently committed by management staff e.g. general managers, managing directors. The victims of this kind of fraud are investors and creditors and this is done via financial statements. Management fraud is driven by the need to acquire more resources from new and existing share capital holders or suppliers. Management fraud may also be driven by the need to create a good corporate

image/standing of the business in the eyes of the regulator or supervisor e.g. Central Bank and Kenya Bankers Association. Management in most organizations is perpetrated through two major avenues: deception and deprivation. Management can overstate its assets or and revenues or understate liabilities and or expenses. ACFE (2011) believes that it is carried out through fictitious revenues, timing difference, improper asset valuation concealed liabilities and expenses and improper or inadequate disclosure (Kingsley, 2012).

### **2.3.2 Employee Fraud**

Employee fraud often referred to as non-management fraud is primarily committed by the employees of the banks (Tchankova, 2012). Employee fraud is mainly characterized by cash theft from bank tills, forgeries of customers signatures with the intention of withdrawing monies from the customer account, opening and operating fictitious accounts and illegal transfer of funds to other accounts (Kingsely, 2012). Employee fraud can also be driven through illegal transfer of funds and assets, false balance crediting, opening, use and management of fictional accounts, claiming of overtime for hours not worked, fund diversion (tapping funds from interest into a suspense account) computer fraud via compromising log in credentials of an e-banking user (Akinyomi, 2012).

ACFE (2009), in their respective studies on fraud in the financial and banking sector noted that staff can also collude to misappropriate organizations assets e.g. cash, inventory customer information. Therefore, banks must take into consideration the location, place and security of assets and the responsible employees for the assets. Common employee fraud schemes include employees creating and paying for non-

existent goods and services, payment of invoices that are inflated or made up, presentation of inflated and fake credit notes, customer list theft and unlawful acquisition of proprietary information (Kingsley, 2012).

Bank staff that have access to tangible assets and the accounting systems that record and track the activities of an employee. However, technologically savvy employees can use the same systems to conceal their identities and theft. This is especially so when the staff establish fake vendor accounts and embed them in the master file to enhance payment processing. Furthermore, employees can steal products or assets of the company and charge the same to the cost of sales which reduces the profitability of the company while asset sales and removal for asset list will reduce the asset of the company (AFCE, 2009). Given the transition to a service based, knowledge economy and more valuable assets of a bank are intangible e.g. customer lists and copy righted material. Intangible assets theft may include the unauthorized copying and use of software and other intellectual property (AFCE, 2009).

### **2.3.3 Third Party Fraud**

Frauds perpetrated by customers and non-customers of banks are outsider fraud. These may include the following:

#### **2.3.3.1 Cheque Fraud**

This is the oldest financial crime. It is the commonest method by which customers and the bank are defrauded. Counterfeit cheques not written or authorized by legitimate account holder, forged cheques where a stolen cheque not signed by account holder, or altered cheque where an item that has been properly issued by the

account holder but has been intercepted and the payee and/or the amount of the item have been altered (Onkagba,1993).

Forgeries is one entrenched mode of fraud where employees forge and copy a customer's signature with the aim of withdrawing funds from the customer's account. The major target accounts for forgeries are targeted savings account, deposit accounts, current accounts or transfer instruments. Experience has shown that most of such forgeries are perpetrated by internal staff in partnership with outsiders with the employees providing sample signatures of the customers (Akinyomi, 2012).

#### **2.3.3.2 Misrepresentations and Impersonation**

Fraudsters make false statements and or submit falsified documents including rent rolls, lien waivers and financial statements to boost loan applications. They may also make fraudulent disbursement requests to receive loan proceeds. This fraud activity may occur across simple banks using multiple accounts by opening an account with false identification (Onkagba, 1993). In impersonation and misrepresentation, the fraudster always assumes the identity of another individual with the goal of committing a fraud or dishonest activity. Impersonation may be done to acquire cheque books to commit fraud or acquisition of cheque leaves for fraud purposes. According to Akinyomi (2012) impersonation is particularly very successful where the outsider works in collaboration with an insider.

#### **2.3.3.3 Money Transfer Fraud**

Money transfer services refers to the movement of financial assets and resources

from one account to another mostly the beneficiary account. Money transfer can occur through mail, telephone or at the counter, mobile phones or through other electronic systems. Money transfer fraud occurs when the beneficiaries detailed are changed or altered to reflect those of a different individual or beneficiary (Onkagba, 1993).

#### **2.3.4 Controlling Fraud mechanism**

An anti-fraud strategy includes elements of prevention, detection, deterrence and response. Business must develop concise and clear strategic responses towards fraud. This will include effective communication on the seriousness of fraud and the probable punitive measures taken due to fraud in the business. Identified cases must form case studies and examples of the stern action taken by the business against fraud. This is one of the most effective ways to combat fraud in the organization (CIMA, 2009).

##### **2.3.4.1 Creating an Encouraging Work Atmosphere**

Positive and good working environments enhance the compliance of employees to established rules, policies and procedures which are set for the success and sustainability of the business. A good working environment enhances communication between employees and management and guarantees positive employee recognition and great reward system. This kind of working atmosphere reduces the levels of internal fraud in the organization (Kingsley, 2012). A workforce culture includes having adequate and sufficient policies, rules, regulations, procedures, protocols and practices human resource management of employees (recruitment, selection, orientation, development, remuneration, career

advancement, motivation, training and termination) to deter fraudulent and corrupt behaviors include practices that deal swiftly with incidents and protect whistle blowers (ACFE, 2009).

#### **2.3.4.2 Ethical Culture**

An ethical culture includes defining principles and values have indicators of high levels of ethics in the organization as well as zero tolerance to corruption and fraud. It also enhances ethical climate and mental notes in the employees not to engage in fraud and corrupt activities. Ethical culture should be incorporated via ethical leadership through rewards and acknowledgement as a model of appropriate conducts in the face factors and behaviours that would promote or motivate employees to engage in fraud (ACFE, 2009).

Attitudes within an organization often lay the foundation for a low or high-risk fraud environment. In a high-risk environment, petty issuers, expense fraud and other minor forms of fraud are overlooked or dealt with leniently. In low risk fraud environment, the business takes serious action on minor or major acts of fraud. In some cases, there may even be risk of total collapse of the organization either through a one act of fraud or very many small acts of fraud. Organizations have come to realize that high ethical standards bring long term benefits as customers and the community realizes that they are dealing with trustworthy organizations. They have also realized that improper, adverse actions, fraud and corruption often cause serious negative impacts to the people and organizations concerned when exposed (CIMA, 2009).

#### **2.3.4.3 Types of Employees**

Cost of hiring dishonest employees cannot be calculated: A dishonest employee destabilize any effort to build a positive work atmosphere and constantly strive to defeat any internal measures. Companies should ensure they conduct a background check that covers criminal history, education, previous employment, civil history for possible lawsuits before employing anyone. The need to hire honest staff cannot be overemphasized (Kingsley 2012). Fraud and business risk in any organization is inherent in the hired employees especially in senior positions where trust and authority are critical. Therefore, it is crucial to conduct due diligence on employees and know them in order to authenticate their competence and credentials.

Furthermore, this is important in knowing the integrity of the employee and how this will influence his actions in the organization. Employee due diligence can be undertaken through confirmation of education qualification, work experience and history and follow up with the references provide. In addition, due diligence may be crucial in acquiring undisclosed information by the employee especially one that may have an impact on the integrity of the employee (ACFE, 2009)

In undertaking employee due diligence, the business must take into consideration the applicable rules and regulations. This is because the rules and regulations guide the conduct and acquisition of the information. Nevertheless, the business can acquire background information of the employee through authorized criminal record survey. Other strategies to acquire information about an employee include acquiring legal counsel on how to conduct and acquire employee information. Due diligence should also be undertaken on bank customers, suppliers and partners to identify any

information with an impact on the financial health, ownership, reputation and integrity which may possess an unacceptable level of risk (ACFE, 2009).

#### **2.3.4.4 Perform Expected and Unexpected Audit**

Unannounced financial audits and fraud assessments should be done regularly. This can help unearth any vulnerability and appraise the effectiveness to the existing controls (Kingsley, 2012). Hillison et al. (1999) found that surprise fraud audits have potential to act as a deterrent to employee fraud. A surprise audit gives perpetrators less time to alter, destroy or hide records and other evidence. Some firms may be reluctant to use surprise, pre-emptive fraud audits because of a perception of adverse employee reactions. Honest employees should be made to understand the importance of fighting fraud. It may be important for management to periodically communicate to employees the importance of audits and also to solicit staff input on how to conduct surprise audits. This may help in reducing suspicion and facilitate co-operation.

#### **2.3.4.5 Enforce Internal Controls**

This is designed to promote operational efficiency, provide dependable financial statistics, protect the assets and records and encourage adherence to prescribed policies. A sound internal control system has features that promote efficiency and effective tracking of transactions and ensuring that all activities are properly authorized, recorded, and reconciled (Kingsley, 2012). An internal control system should have all principles and procedures that support the organizations effective and effective operation. They deal with things like approval and authorization procedures, restrictions and control over transactions, reconciliation of activities and



accounts and provision of security to assets. The number of internal controls that an organization can have depends on nature and size. Internal controls minimize fraud. Examples of such controls may include requirement of multiple signatures for high value transactions, restriction belongings that can be brought into an office and conducting random searches.

As part of the risk management framework, the organization must review the internal controls and ensure that any weaknesses in the internal controls are addressed. Furthermore, the organization has the responsibility of ensuring that internal controls are assessed and updated to meet global trends and best practices constantly. This reflects good practice. Finally, these internal controls should be entrenched within the organization culture and operations (CIMA, 2009).

#### **2.3.4.6 Compensation Programs**

It is a human trait to want recognition and reward for positive performance and success. Continuous and rigorous assessment of employee's performance, coupled with constant, timely and effective communication to the employee on the performance assessment has a huge bearing on the reduction of fraud. As part of the employee assessment process the organization must recognize and if possible, reward any accomplishments of the employees, especially those whose performance require so.

Furthermore, employees must feel that the reward is of value to them. Failure to do so will lead to guilt feelings, low motivation and demoralization of employees which might create rationalizations for acts of fraud. Market research and surveys

must also be done by the organization to identify whether the remuneration and compensation of employees is adequate, motivating and in line with industry trends. The findings of the survey will also be instrumental in striking a balance between the use of fixed and variable compensation. It is good to note that if compensation is based on compensation for short term performance, managers maybe motivated to cut corners or fabricate financial results to achieve those bonuses (Hillison, 1999).

#### **2.3.4.7 Establish a Fraud Policy**

Every bank should have an approach to deal with fraud. The approach should be clearly stated in the fraud policy. This is established to facilitate the implementation and actualization of internal controls which will aid in detection and prevention of fraud against companies. The must be applicable to any wrongdoing, or suspected misdeed, involving all stakeholders in the business (Pacini, 2009). A fraud policy should have a scope, what actions constitute a fraud, the unit responsible for investigations, confidentiality clauses, and an authorization for investigating suspected fraud, reporting procedures, and termination procedures. A bank fraud policy should be separate and distinct from a corporate code of conduct or ethics policy. It should be clearly communicated to all employees through new orientation of new hires, annual training seminars and annual performance evaluations. It is important to have a written acknowledgement by each employee that the policy has been read and understood as required as stated by (Sinason, 1999).

#### **2.3.4.8 Establishing a Telephone Hot Line**

CIMA (2009) notes that a dedicated and confidential 24/7 hotline to report fraud is one of the most effective strategies to combat fraud. The hotline must be strictly

confidential and will greatly aid the company's efforts to detect fraud. Indeed, studies have shown that most losses in an organization are caused by the ignorance of small signs and lack of fraud detection strategies. In addition to installation of a telephone hotline, every member of the organization must be aware that it is his/her responsibility to report any kind of fraud or irregularity in the business. Therefore, the hotline must have inbuilt facilities that ensure that the identity of the reporter is not revealed whether by choice or default (CIMA, 2009).

Anonymous tips received through hotlines are an effective strategy and channel to detecting fraud. The hotline should be utilized to create awareness, ensure ease in use and prompt actions on reports on the hotline. Education of employees on the use of the hotline is also important since they are the source of information. To enhance the efficiency of the hotline it must be manned by a qualified and experienced employee who has multilingual abilities and is available 24 hours a day, 365 days a year. Once a fraud has been reported via the hotline, it would be important to let the whistle blower know that timely action will be taken. It would be important to analyse collected data against the industry norm. Hotlines may be supported in-house or provided by a third party (ACFE, 2009).

### **2.3.5 Fraud in International Countries**

Fraud is an area of convergence for financial firms. Tech experts and young employees are leading the proliferation of insider fraud across most businesses in the work. This is opposed to insider fraud driven by supervisors, managers and superiors in the business. This has led to the ranking of fraud as one of the top five concerns for both banks and insurers in East Africa (PricewaterhouseCoopers [PwC], 2011).

Institutional trust plays significant role in fraud detection and prevention. Modern business especially those operating online are using the principles of institutional trust, to improve and enhance effective governance as a strategy towards reducing fraud.

The study of fraud encompasses criminology, psychology, accounting, auditing, and management. According to Wels (1997), fraud growth and rise can be explained through a model that consist of three major factors: personal pressure, availability of opportunities and rationalization of the act/attitude. The Fraud model has its roots in the research noted by criminologist Donald Cressey. According to Cressey (1973), a sharable financial need is crucial to understanding behaviour of one who violates trust to commit fraud. What is deemed non-sharable is in the eyes on the offender.

Other factors that lead to the increase and proliferation of fraud include: lack of experience and expertise in fraud detection, IT savvy employees, change resistance by superiors and older generations, lack of professionalism and competency in recruitment and selection of employees, poor and rigid judicial systems and procedures, small fines and court rulings that do not deter fraudsters and lack of effective communication and coordination of fraud tracking, detection and prevention by banks across the country (PwC, 2011).

In addition to financial loss incurred by banks, the financial cost incurred arising out of court cases should encourage banks that to detect fraud in time to save money as well as damage to the bank's credibility. In Europe banking sector, fraud has also hit

major banks and shows millions of euros being lost in every year. The fraud in ATM machines and other electronic banking systems have led to bank getting losses in every year. The figure above shows the report, which was compiled by the Euro-system, namely the ECB and the 17 national central banks of the euro area (with data from 25 card payment schemes, including the most well-known card brands, banks and other large national issuers), looks at fraud using different kinds of cards (debit and credit) and according to type of usage. In 2011 some 56% of the value of fraud resulted from card-not-present (CNP) payments ó i.e. payments via post, telephone or the internet ó while one-quarter resulted from point-of-sale (POS) terminals and about one-fifth from automated teller machines (ATMs). (ECB,2014).

A survey was done by PWC on 33 banks in Kenya, Tanzania, Zambia, Rwanda and Uganda participated in the late 2011 and 2010. In this study, the researchers sought to identify the risk identification and risk readiness levels in most local businesses. Over 50% of the respondents to the study indicated that fraud as an area they needed to put more effort in preparedness (PwC, 2011). Furthermore, the economic survey of 2010 by PwC found that fraud incidents and cases had increased with higher margins in the year 2010 than in any other preceding year.

Approximately, 90% of the respondents to the study indicated that most businesses in East African region had recorded some cases of fraud while banks in the country had lost over TSh 38 billion with just three months, August to October, 2010. This growth in the banking fraud was grounded on the rapid growth and expansion in banks which necessitated the implementation of complex multiple technological systems that promoted levels of fraud (PwC, 2011). Furthermore, the effectiveness

of internal control systems in most banks is diminishing in comparison to the boldness and skills of highly networked and sophisticated fraudsters (PwC, 2011).

### **2.3.6 Bank Model**

The theoretical framework found in this research about factors affecting Electronic fraud in the banking operations will look on 3 model being used in the banking operations and how they can assist in controlling fraud in the banks.

#### **2.3.6.1 Non-bank-led Model**

The non-bank-led model usually excludes the bank from the overall presence and presents Telecommunication industries to execute all the functions. The non-bank-led model helps banks to play fewer parts in customer's daily transactions, the bank only provides a security layer in the fund's allocation. The main challenges in this model are how you can ensure flexibility between customers and operators (agents) which includes other factors such as affordability and reliability. (Infogile Technology, 2007). This conditions mostly help the bank to detect fraud easily since most of the works are done by 3<sup>rd</sup> Party company, and the bank works effectively.

#### **2.3.6.2 Bank-led Model**

This model separate components found in a conventional bank and be able to manage all the transactions with all the agents via digital devices instead of bank branches. Bank-led Model ensure the increase in the financial network by utilizing different channels that are cost effective compared to that provided by the banks. Inside this model, the outside reach creates a joint venture with certain bank according to certain agreements, however, the confidentiality of customers is

protected by the bank. (Infogile Technology, 2007). The best way to fight fraud in the bank is through the joint venture between the companies, most banks hire security to make sure the fraud in both management and employees' side doesn't affect daily operations.

### **2.3.6.3 Bank-Focused Model**

According to (Infogile Technology (2007), this model is accessible when banking institutions use non-traditional means channel to enable transactions to its clients such as using of internet banking or electronic banking including ATM Machines to provide banking services. The bank-focused model allows customers to access low-cost delivery. The underlying innovative technology delivers banking services but mostly these services are somehow limited and, therefore, are termed as low-cost delivery. This is the most passage that fraud is being detected daily as customers are not aware of the fraud mechanisms in ATMs and other third-party peoples. Tanzanians banks are focused mostly on this model which resulted in many problems at the moment. This research had exploited the problems and had try to come up with solutions.

## **2.4 Empirical Literature Review**

An empirical review is a summary of research on certain topic and their explanations related to same research area done by other researchers. In this research the author had look to learn what other researchers have done in the area of factors influencing electronic fraud in different banking sectors around the world.

### **2.4.1 Empirical Literature Review Worldwide**

From the study done by (Ashu,2009) which examines the issue of frauds from the

perspective of banking industry. The study seeks to evaluate the various causes that are responsible for banks frauds. It aims to examine the extent to which bank employees follow the various fraud prevention measures including the ones prescribed by Reserve Bank of India. It aims to give an insight on the perception of bank employees towards preventive mechanism and their awareness towards various frauds. The study signifies the importance of training in prevention of bank frauds.

A strong system of internal control and good employment practices prevent frauds and mitigate losses. The research reveals that implementation of various internal control mechanisms are not up to the mark. The results indicate that lack of training, overburdened staff, competition, low compliance level (the degree to which procedures and prudential practices framed by Reserve bank of India to prevent frauds are followed) are the main reasons for bank frauds. The banks should take the rising graph of bank frauds seriously and need to ensure that there is no laxity in internal control mechanism

In a study by Pan (2012), they concurred with other scholars on fraud that the use of the fraud triangle and other fraud frameworks are crucial in developing a conceptual model for the study and research on fraud. The financial markets have become innovative, creative as well as complex which has presented opportunities for fraud. While the research and recommendations by Pan et al. (2011), were undertaken in the European continent, very few studies have focused on fraud management and prevention in the African region and especially the East African region. With regards to fraud issues in Saudi Arabia, Mams (2013) relayed his experience with bank employee defrauding customers of the bank where he works. When arrested and



tried, more than thirty million riyals was traced to have been falsely acquired by the culprit. Similarly, Abdullah (2012) study pointed out the need for banks to be alerting customers about confidential and business or personal information in all their dealings, and also by maintaining the confidentiality and integrity of their company or personal data in order to prevent fraud.

Extreme cases of bank fraud have the potential to highly disturb the economic system of a country. For example, in 1983, the Tel Aviv Stock Exchange (TASE) closed for 18 days following earnings management frauds attempts by the six main banks during a period of unusually high sell-offs (Blass & Grossman, 1996). The Turkish banking crisis of 2000 was also found to have likely been caused by systemic banking fraud, including the use of back to back loans intended to circumvent lending and capital requirements regulations (Soral et al., 2006).

Afayi (2014) examined the effect of fraud on the performance of banking industry in the United States of America (USA). Banks as a whole was examined, give answers to why bank failed, examined how many banks have failed or what percentage of banks have failed in USA as a result of fraud, scrutinized the protective measures the banking industry have taken to prevent fraudulent practices and list any corrective action if need be. The study spanned from 2000-2014 in which about 523 banks have failed throughout USA.

In method 1, the ratio of bank failure caused by fraud as opposed to other factors- out of 20 selected banks, 8 banks representing 40 percent failed due to fraudulent practices. Ganesh and Raghurama (2008), believe that training improves the

capabilities of employees by enhancing their skills, knowledge and commitment towards their work in the survey conducted by them, about 80 executives from Corporation Bank and Karnataka Bank Ltd of India, were requested to rate their subordinates in terms of development of their skills before and after they underwent certain commonly delivered training programs.

Responses revealed that for the seventeen skills identified there was improvement in the skills statistically. The paired t-test was applied individually for the seventeen skills, and all these skills have shown statistical significance. The seventeen skills include analytical skill, human resource skill, marketing skill, communication skill, accounting skill, credit appraisal skill, cash management skill, time management skill, inter-branch reconciliation skill, conceptual skill, information technology related skill, technical skill, role identification skill, problem solving skill, behavioural skill, risk management skill and customer service skill.

#### **2.4.2 Empirical Literature Review in Africa**

A study by Odi (2013) investigated the exposure of fraud among Nigerian banks, and the results showed the considerable involvement of employees and customers in fraud and fraudulent practices. This results as an African country share similar outcome with the most countries in the world. As Hoffmann (2012) observed, there is an association between customer familiarity, knowledge about fraud prevention measures, relationship quality and customer loyalty. Primarily, it pointed out that the positive relationship between customer familiarity and knowledge of fraud prevention and its measure eventually results in customer loyalty, which in turn influence continuous patronage of the products from the bank. Thus, they point to

the significance of fraud prevention, and the value of building customer loyalty through it.

A study of banking governance in Ghana found that there were considerable problems with corporate governance and fraud (Evans & Dadzie, 1998). This research, from the records of the Central Bank of Ghana during the 2000s showed that informed lenders charged higher fees for their loans (indicating potential bribes or other corrupt activity), and that prior relationships between lending officers and borrowers reduced enforcement of loan terms. This research does not provide a clear indication of corruption, although this was presented as one of the possibilities; it also suggested that lack of information or informal collection practices were evidence, as well as corruption in the general institutional structure.

In terms of fraud detection and prevention in African banking, evidence is scarce. However, one study showed that Nigerian commercial banks used relatively few risk management practices when engaged in information systems outsourcing (a potential source of external fraud). This study indicated that strategic, management, and information systems approaches were used only lightly in these banks, indicating a serious lack in comparison to international banks, along with little regulatory attention to information technology (Adeleye et al., 2004). This both decreases competitive ability and increases fraud. Fraud innovations such as the Nigerian or 419 frauds, which commonly involves fraudsters using email to contact strangers, claiming to be sons or daughters of African diplomats, businessmen or other notables and extracting money due to implausible claims of large amounts of money, has made it clear that many African countries do not have sufficient fraud controls in

place (Ampratwum, 2009).

Adding to that, another research done by (Wekesa et al. 2016) regarding analyzation of the determinants of effective fraud management in domestic tier one commercial banks in Trans Nzoia County. The analysis was focused on the domestic tier one commercial banks in the County as the population of the study. The study was guided by the following objectives; to analyse the effect of the independence of the internal audit personnel, the competence of the internal audit personnel, the presence of the internal audit charter and the management support as determinants of effective fraud management in the domestic tier one commercial banks. The study was guided by the agency theory, the fraud management lifecycle/theory and the communication theory. A correlation research design was adopted in which an in-depth study of the determinants of effective fraud management was carried out from the target population of the senior management staff and the internal audit personnel in the domestic tier one commercial banks in the County.

The survey targeted departmental heads in the banks by employing census method. The source of the required data was through the questionnaires, covering both qualitative and quantitative data, administered to the target population by the researcher. The findings revealed that the regression effect is statistically significant and indicated an accomplished prediction of the dependent variable, better than if done through chance through the F calculated ( $F = 12.2896$ ) which was greater than 5% level of significance that showed the overall model was significant where the Internal Audit Independence explained 11% of EFM, Competence of Internal Auditor Personnel 46% of EFM, Presence of Internal Audit Charter 12% of EFM,

and Management Support explained 16% of EFM within the domestic tier one commercial banks. However, Competence of Internal Audit Personnel was the most significant predictor (determinant) of EFM at 46% with ( $\beta = 0.086$ ).

Another study done by (Ojeaga, 2014) whom investigates factors that incite fraud in the banking sector in Nigeria, using times series data for fraud obtained from CBN data from 1998 to 2010. It was found that high bank deposit was primarily responsible for a high-rise fraudulent occurrence in the Nigerian banking sector particularly management fraud, some other factors that were also jointly responsible for these occurrences include high interest rates, low commercial bank lending and poor oversight function by the Central Bank and other financial regulatory agencies.

The method of estimation used in the study is the quantile regression estimation method which is a non-parametric estimation method based on the premise that the sample median had tend to that of the distributional median, it presents some obvious advantages over OLS (ordinary least squares) estimates, since the results are robust in the presence of outliers and heteroscedastic errors in the response measurement and allows for the exploration of other central tendencies and statistical dispersion properties of the dataset Machando and Silva (2013). The results are robust even after controlling for presence of heteroscedastic error in the response measurement as well re-sampling the dataset (conducted by the bootstrapped quantile regression technique). Further explanation is also provided for the implication of variables identified to drive fraud occurrences using kernel density estimation.

### **2.4.3 Empirical Literature Review in Tanzania**

Few researches have been conducted in Tanzania regarding fraud detection and prevention. This is a major challenge on getting the literatures which has been done in Tanzania. A study done by Leonard (2013) which was conducted at the CRDB Bank and NMB Bank Public Limited Companies at headquarters and branches located in Dar es Salaam. The study was on assessment of fraud and its management in commercial banks in Tanzania.

The specific objectives of the study were to analyse the nature/ types of frauds in banks and establish why fraud occurs. Some classes of frauds in Tanzania commercial banks revealed were frauds related to overstatement of collateral value when customers applied for bank loans. Frauds related to manipulation of foreign exchanges and ghost loans- loans issued against forged collaterals. Internal controls were found adequate in some areas/ processes, however were not effective. In some areas/ processes where controls were adequate were not effective as sometimes management tends to override them to commit fraud. In some instances, the areas highlighted by independent reviewers such as auditors for improvement, management of banks did not implement some of the recommendations provided by independent reviewers.

On impact, it was revealed that banks suffered both financial and non-financial impacts. For financial, it was established that trend and magnitude of fraud is increasing yearly and mostly committed by staff non-management level, sometimes by colluding with external parties. For the past three years the two big banks suffered losses approximately to TZS 5,002.85 million (2010), TZS 5,474.95 million

(2011) and TZS 8,893.25 (2012) respectively due to frauds. Based on the results of the study, the researcher concluded that fraud still occurs in banks due to weakness in internal controls, management overriding the established controls, low remunerations to employees and lack of fraud threshold for management accountability despite who caused the loss.

These factors amount to opportunity, pressure and rationale which are fraud triangles. To address the weakness noted, the researcher recommended that bank management to ensure controls are adhered to, survey on salary should be done in order to commensurate with job responsibilities and fraud threshold to be established by both bank management and regulator. It was also recommended that, bank regulator to initiate formation of special courts for recovery of money fraudulently obtained from banks in order to relieve commercial banks from losses.

New data shows fraud is raising its ugly head in Tanzania's banking industry, with techno-savvy criminals colluding with bank employees to siphon millions of shillings out of customers' accounts. Police records show that between 2010 and the first quarter of 2013, cyber fraud-related losses in banks stood at around TSh 9.8 billion (\$ 6.10 million). The police cyber-crime unit said between 2011 and 2012, at least 500 Tanzanians were arrested over fraud cases. Some 320 people were arrested between July and December 2011, whereas in 2012 about 230 people were arrested over the crime. (Corporate digest, 2013). According to then Deputy Minister of Finance, Saada Mkuya, "cyber-crime is becoming an economic disaster, prompting the state to fast-track the performing of the cyber-crime law. "Looking beyond the numbers, cyber fraud spells economic disaster not only for bank customers, but also

for the financial institutions, mainly banks, she said.

Another mentioned research done by (Masamila, 2014) in regarding security issues with the state of mobile banking in Tanzania. Mobile technology offers an unprecedented growth opportunity for banking industry in Tanzania. As the economy continues to prosper, increasingly affluent consumers and underbanked segments create demand for new financial products and services. Many consumers in Tanzania have mobile phones, but not bank accounts. Therefore, the mobile channel presents an effective way to connect them to the national financial grid. For the local banks, going mobile may increase banks opportunities to unlock the inherent potential of underbanked segments. This paper addresses the current state, future prospects, and security challenges to the usage of mobile banking in Tanzania. The findings of this paper show that the need for the government and other financial sectors to make the security is strengthened in order to maximise mobile banking usage in Tanzania.

## **2.5 Research Gap**

Existing literature is concentrated in the West African region especially in Nigeria with scarce studies in other regions in Africa. This has created a shortage in empirical evidence and studies on the local scene. While fraud has been identified as a major challenge and issue in the Tanzanian banking sector (Kalimangasi, 2014) very few scholars or studies have sought to establish the causes and strategies to combat fraud in the financial sector. This may have had a negative impact on policy making as policy solutions to fraud were not necessarily informed by empirical evidence. This research tends to fill the void on examining the fraud cases found in

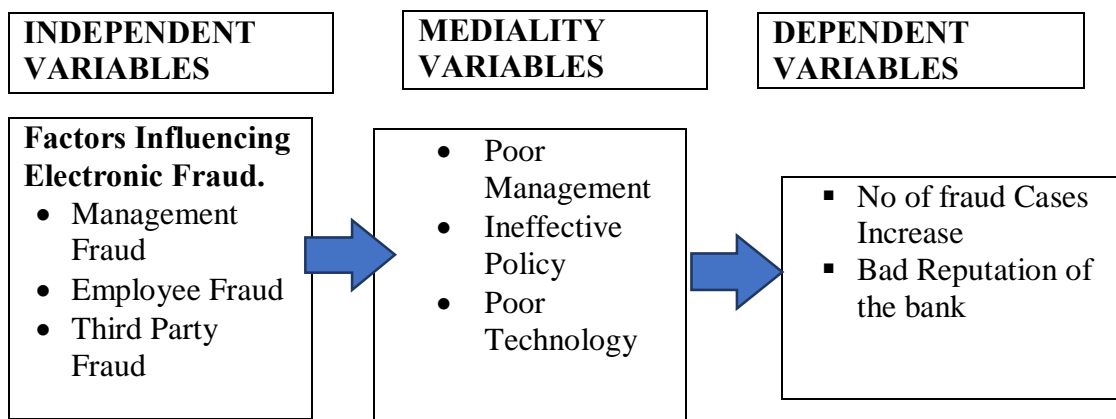


Tanzania and the way to combat them.

## 2.6 Conceptual Framework

The concept is an abstract or general idea inferred or derived from specific instances.

A concept is a word or phrase that symbolizes several interrelated ideas. Unlike a theory, a concept does not need to be discussed but to be understood (Collins et al., 2011).



**Figure 2.1: Conceptual Framework**

**Source:** Researcher's Construct, 2019

## 2.7 Theoretical Framework

Theoretical framework is a conceptual structure in the form of a visual aid or a document that is used to explain the concepts, key factors and variables used in the study and to represent the apparent relationship between the variables in the study (Miles and Huberman, 1994). The theoretical framework below tries to explain the relationship between dependent variable and independent variable. Dependent Variable is the output variable you are really interested in monitoring to see if it was affected or not. It can also be called the "measured variable," the "responding variable," the "explained variable,". Independent Variables: These are the individual

variables that you believe may have an effect on the dependent variable. They are sometimes called "explanatory variables," "manipulated variables," or "controlled variables." (Miles and Huberman, 1994). In this research, poor management or less control of staff will lead to fraud to happen and therefore number of frauds cases will increase in People bank of Zanzibar Limited.

Adding to that ineffective policies in recruitment and working conditions inside the banks will also increase the fraud cases in employees of the bank and this might also increase number of fraud cases in the bank. And lastly, poor technology inside the bank, that can lead to cyber-fraud inside the banks will also increase the number of fraud cases inside the People bank of Zanzibar (PBZ). When all this happens, they will lead to change of performance of the bank in customers perspective because most of them they will leave the bank and give bad reputation to the whole bank. This research tried to understand these challenges in People bank of Zanzibar and suggested a better way of combating fraud in PBZ.

## **CHAPTER THREE**

### **RESEARCH METHODOLOGY**

#### **3.1 Introduction**

This chapter details the methodology the researcher used in studying and collecting data on theme "Factors Influencing Electronic Fraud in Banking Industry in Tanzania". It includes the areas of study, research design, target population, sample size and sampling technique, types and sources of data, data collection methods, validity issues, and data analysis methods in order to respond the research questions.

#### **3.2 Research Design**

A research design is a logical outline on how to conduct the research, how to answer research questions, how to deal with the study, how to connect empirical data to initial research questions as well as conclusions (Yin 1994:19 in Scholz 2008:49). Therefore, a research design and methods applied must be chosen carefully to which assists in formulating a significant knowledge and artefacts to a particular problem. In this case therefore, a research design had involved measurement, classification, comparison, and interpretation of data and it not confined on only data collection.

There are two main types of research approaches namely qualitative and quantitative research, which have different underlying assumptions. Quantitative research is designed to adopt an objective approach of obtaining required data in an investigation. The approach therefore ensures that only required facts are obtained through quantification of the data which becomes measurable and subject to scientific principles. Quantitative approach is therefore more suitable to examine cause effect relationships of variables in natural sciences. The approach is therefore

associated with statistical analysis for inferential and descriptive reports of study phenomenon (Bryman, 2001). This research has used the quantitative research method with the use of questionnaire derived from past researchers and was used to collect the data in the PBZ bank with only few knowledgeable workers were given the questionnaire to respond.

### **3.3 Area of the Study**

The study was conducted in People bank of Zanzibar Ltd with the concentration given to those departments which deals with a lot of transactions whereby there is a room of fraud detection. Departments such as accounting, Human Resource, Audit and IT sections, were all given questionnaires in order to understand the nature of the problem and on how to combat the issue at hand. Since the banks has many branches in Tanzania including Mtwara, Dar es Salaam and Zanzibar. This research had solely focus on those departments found in Zanzibar.

### **3.4 Population of the Study**

A research population is generally a large collection of individuals or objects that is the main focus of a scientific query. It is for the benefit of the population that researches are done. However, due to the large sizes of populations, researchers often cannot test every individual in the population because it is too expensive and time-consuming. This is the reason why researchers rely on sampling techniques In this research the population of the study are all bank staff that are working inside People bank of Zanzibar limited in different branches in Tanzania, the total number of workers in PBZ ltd as of 2016 are 304 staff, but since due to the population being too vast and the author cannot reach all the staff at the same time due to many

reasons including geographical locations and the scope of the research, so sampling was used for this study.

### **3.5 Sampling Design and Sample Size**

#### **3.5.1 Sampling Design**

The purposive sampling technique is a type of non-probability sampling that is most effective when one needs to study a certain cultural domain with knowledgeable experts within. Purposive sampling may also be used with both qualitative and quantitative research techniques. The main goal of purposive sampling is to focus on particular characteristics of a population that are of interest, which will best enable you to answer your research questions. In this research the selection of respondents was considered to measure the factors influencing electronic fraud in Tanzania. This method was based on the judgment of the researcher regarding the characteristics of representative sample. The cases were selected due to their uniqueness and the type of banking operation that have been undergoing in Tanzania.

#### **3.5.2 Sample Size**

Sampling refers to the selection of subjects or unit of analysis. In qualitative or quantitative research, the selection of the subjects is largely dependent on the purpose of the study hence the term purposive sampling. There is no singly acceptable number of participants to be considered in a quantitative case study research enterprise, it all depends on the one the author think can settle the demand of the research. For instance, Cresswell (2008) suggested for between 5 to 25; Adler, Baker & Edwards (2012), chose from 12 to 60 and 30 being the mean; Glaser and Strauss (1967) sees saturation to be the point of diminishing return i.e. when the data

has started repeating itself.

From the above consideration, the author had considered (Baker & Edward,2012) to use a sample of 30 banking experts that were chosen as a sample for questionnaires to represent the population under study. The sample were selected basing on the convenience for the subject matter meaning that the banking officials have a great knowledge of the technical issues related to the factors influencing electronic fraud in Tanzania, as they have greater accessibility and once the technology is adopted, they are first users before the customers acquire the given knowledge.

**Table 3.1: Research Sample Size**

DEPARTMENT	No of PBZ staff
Accounting & Finance	<b>10</b>
Banking & Customer Care	<b>7</b>
HRM	<b>3</b>
ICT	<b>8</b>
LOAN	<b>2</b>
Total number of respondents from department	<b>30</b>

**Source:** Research Data, 2019

### **3.6 Data Collection Methods**

Yin (1994:79) provides an overview of six methods that are used in data collection and these are: interviews, direct observation, documentation, archival records, participant observation and physical artefacts. Also, he noted that the list may however go beyond the six mentioned sources to include others such as films, photographs, videotapes, street ethnography and life histories. Kothari (2004) stated that there are numerous techniques of collecting data, such are observation method,

interview method, questionnaires, just to mention but a few. Secondary information was obtained through literature review, mainly to

- i. Establish the existing knowledge base with respect to research issued at hand,
- ii. Supplement primary data collected via direct link of work personnel. It was therefore used to corroborate critique and fill knowledge gaps in areas not sufficiently covered by the primary data sources.

Primary data collection was done via work personnel in quantitative nature. The primary data for the research was extracted from a survey that was conducted in PBZ bank in Tanzania where a total of at least 30 respondents participated in the research. The demographic profile of respondents can be seen in the next chapter of this document. This method is adequate enough for data collection while making projections within the research. Whereas secondary data collection is done from articles, research papers, journals, and business websites that relates with mobile banking and telecommunication adoption.

### **3.7 Data Collection Tools**

The questionnaires were gathered from the banking focus model used by (Yee 2008). The questionnaire was divided into sections where it can be divided into more subsections. The five-point Likert scale ranging from 1-strongly disagree to 5-strongly agree was used for the questions to indicate a degree of agreement or disagreement with each of a series of statements related to the stimulus objects. The first part was used in gathering respondent's basic information. The second part of the questionnaire focused on getting information on perception of fraud in PBZ bank Limited which uses the Likert scale. The following third part of the questionnaire

tried to gather information on types of fraud seen on the bank, and they were graded using High, Average, Low and no Effect scale. And finally, the last part which is prevention of the fraud had used the scale of very effective, effective, least effective and no effect.

### **3.8 Reliability and Validity of Data**

In the process of data collection, the researcher had ensured that the data obtained from questionnaires and documentation is correct, valid and reliable.

#### **3.8.1 Data Reliability**

Reliability is concerned with estimates of the degree to which a measurement is free of random or unstable error. It refers to the relative level of consistency, stability, dependability and accuracy of constructs (Rahman,2014). It is a contributor to validity and is a necessary but not sufficient condition for validity. A measure is considered reliable if it would give the same results over and over again (assuming that what is being measured is not changing). For this study test-retest method was used to assess reliability where some respondents were revisited to ensure consistency of the responses and the results indicated that the instruments used in the study was reliable.

#### **3.8.2 Data Validity**

Validity refers to the extent to which a test measures what was actually intended to be measured. In measuring the content of validity, some questionnaires were given to a group of experts (five by number) carefully selected during the pilot study to judge how well the instrument met the standards (Noralina,2015). The



questionnaires were modified if they had some changes, which then were distributed to the respondents. By doing so, it made sure validity of the instruments was met.

### **3.9 Data Analysis**

Data analysis refers to the inspection of data obtained from survey or experimental method by making deduction and inferences. These inspections involve uncovering underlying structures, extracting important variables, detecting any abnormalities and testing the assumptions. Collected data are then processed and analysed based on the laid down processes for the purpose the research plan. Data analysis is important for scientific study to ensure that all relevant data are collected for obtaining anticipated analysis and comparison. Processing of data include editing, coding, classification as well as tabulation of data obtained.

After data collection, the data are then structured and summarized in such a way they can be interpreted for a given purpose. Data collected are then presented into tabular and other forms of analysing of data. Quantitate techniques was used for data analysis before they could be tabulated and investigated using a statistical software package known as Statistical Package. Type of analysis methods was purposively method and selective method to analyse better the results. The findings are illustrated in the following chapter (Chapter 4).

### **3.10 Ethical and Legal Issues**

Noted by (Walton, 2012) ethical, social, legal and political issues are raised up by a type of research that involve human subject or participant. Research ethics is mostly focused on the analysis of ethical issues raised by people concerned. Three

objectives are involved in research ethics; the first and comprehensive objective is to protect participants. The second objective is to ensure that a research is conducted in such a way that satisfies individuals, groups and/or society as a one. And the third objective is to examine specific activities and projects for their ethical trustworthiness and observing issues such as management of risk, protection of privacy as well as the process of informed assent

The research process is adopted based on the accordance of ethical standards that govern institution and organization every day. A request to PBZ with an official introduction letter to the management was firstly made by the researchers alongside the research questionnaire, should the request return positive from the bank administration, the researcher is then allowed to conduct the research by collecting data related to electronic fraud in People bank of Zanzibar. During data collection the researcher ensured ethical soundness and confidentiality of data to the respondents. The researcher was required to protect interest of the individuals and groups so as to avoid biasness in data collection. As most financial institutions do not always show all the necessary information to the public, the researcher ensured the host institutions neither exposing confidential information nor jeopardizing the bank status.

## CHAPTER FOUR

### DATA ANALYSIS

#### 4.1 Introduction

This chapter presents the findings of the study on fraud in the banking sector. The findings are deduced from the data collected, analysed and presented in this chapter.

#### 4.2 Demographic Information

This section presents the background characteristics of the respondents

**Table 4.1: Demographic Information**

Variable		Number (N)	Percentage (%)
GENDER	Male	17	56.7
	Female	13	43.3
AGE GROUP	18 - 30	19	63.3
	31 - 50	7	23.3
	51 - 60	4	13.4
	60 and above	0	0
EDUCATION LEVEL	Diploma	1	3.33
	Degree	14	46.67
	Postgraduate	15	50.0
ROLE (POSITION)	Senior manager	3	10.0
	Manager	4	13.3
	Auditor	4	13.3
	Operations/Clerks	19	63.4
EXPERIENCE	1-5 Years	8	26.7
	5-10 Years	10	33.3
	Above 10 Years	12	40.0

**Source:** Research Data, 2019

##### 4.2.1 Gender

Gender balance as one of contemporary issues is indicated on table 2 of the respondents. It is important to give classification of gender group as the later has certain implication in making decision in any institution. Therefore, it was important

to the researcher to obtain a balanced figure between male and female of the surveyed respondents. Fifty-six-point seven percent (56.7%) of the respondents to this study were of the male gender, while 43.3% were of the female gender. These findings imply that the population of study was characterized by a higher proportion of the male than the female gender, although not in huge range of differences. This is revealed in table 4.1.

#### **4.2.2 Age**

The respondents to this study were spread out across various age brackets. However, the 31 ó 50 age brackets represented the biggest proportion of respondents (63.3%). Respondents between the ages of 18 ó 30 were 23.3% while those of the ages between 51 and 60 were 13.3%. This is shown in table 4.1.

#### **4.2.3 Education Level**

Using table 4.1, majority of the respondents of PBZ bank shows 50 per cent of 30 respondents have postgraduate holders while 46.7 per cent of the responses were holding first degree and only 3.3 per cent were holding diploma level. Response to the question on the education level of respondent ñs reveals on how the management and staff of the banking industry can make the choice and decision regarding to the type of electronic banking they had opt to adopt and at what level they are motivated on acquiring and utilizing the mobile banking technology in banking sector.

#### **4.2.4 Role at Work**

Majority of the respondents to this study were Operations Assistant/ Clerks (63.3%). This is because it's easier to get day to day people who are really working on the

banking sector or dealing directly with the customers so that to understand exact problems. Furthermore, both manager/Supervisor and Auditor/Risk Manager have 13.3% each which shows that management also took part in this questionnaire. Adding to that 10.0% of the respondents were senior managers. This data is shown in table 2. These distributions of respondents ensure validity of findings since all workers working in different categories(sections) of the bank responsible for the detection and reporting of frauds.

#### **4.2.5 Experience**

As seen in table 2, forty percent of the respondents to this study out of 30 people had an experience of above 10 years, 33.3% of 30 responders had experience of between 5- 10 years while 26.7 % of 30 responders had experience of 1- 5 years. Working experience has a great importance to stability of the bank and detection of fraud cases through years, but it's also a reason of fraud cases if they work together for a very long time in one department. This is where the shuffling is required in banks.

#### **4.3 Perception of Fraud in PBZ Bank Limited**

Respondents to this study disagreed that PBZ had been successful in fighting fraud in their bank with a mean rating of 2.833, mode of 2 and it is significantly at a 2-tailed scale. This shows that PBZ ltd have a work to do in their hands by making sure they are paying more attention to understand their problems on why they are not fighting fraud in the required way, so that to increase profitability in their banks. In addition, respondents disagreed that PBZ limited was up to date with emerging trends in fraud (mean of 2.667 and a mode of 2). This is also a major concern since

technology is growing very fast in the world and new ways of committing fraud is being done in different styles in the world, PBZ should focus to have international consultants to be taught ways of fighting frauds in their bank.

Respondents agreed that fraud policy is well communicated in PBZ limited to all departments and agree by mean of 3.267 and mode of 4. In any bank, policies, rules and regulations are very important to be followed by all workers in order to improve efficiency of customer services in all departments. The results show that policy is well structured in the banks but there is a room of improvement. Lastly responders agreed PBZ Ltd gives importance to fraud incidences in the bank at all times by having a mean of 3.967 and a mode of 4. This is a good sign to the bank that they embedded the culture of being alert and fighting fraud quickly in their bank which is a productive mentality to the growth of the bank. This is as shown in table 3.

**Table 4.2: Perception of Fraud in PBZ bank Limited**

Perception of fraud in PBZ bank Limited Variables	Test Value = 0					
	t	Mode	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
PBZ Ltd has been successful in fighting fraud in their bank	19.607	2	.000	2.833	2.54	3.13
PBZ Ltd is up to date with emerging fraud trends in the banking industry	16.521	2	.000	2.667	2.34	3.00
Fraud policy is well communicated in PBZ Ltd to all departments	24.189	4	.000	3.267	2.99	3.54
PBZ Ltd gives importance to fraud incidences in the bank at all times	28.404	4	.000	3.967	3.68	4.25

**Source:** Research Data, 2019

#### 4.4 Management Fraud

Management fraud in PBZ ltd was mainly manifested in the form of Understatement of expenses with a mean rating of 3.07. This was the highest observation in the ratings on a scale of 1 ó 4. Other forms of management fraud in PBZ ltd in their descending order of prevalence were: understatement of liabilities (2.30), overstatement of assets (2.20) and overstatement of revenues (1.90). This is a slight concern to the management and the board of directors to make sure all the cost and spending of the management are well documented and presented in the well manner in order to reduce fraud in the People bank of Zanzibar limited. This is as shown in the table 4.3

**Table 4.3: Management Fraud**

Management Fraud variables	N	Minimum	Maximum	Mean	Std. Deviation
Overstatement of assets	30	1	4	2.20	.805
Overstatement of revenues	30	1	3	1.90	.712
Understatement of liabilities	30	1	3	2.30	.794
Understatement of expenses	30	2	4	3.07	.740
Valid N (list wise)	30				

**Source:** Research Data, 2019

#### 4.5 Employee Fraud

Employee fraud was mainly in the form of cash theft in the bank with a mean rating of 1.42. Other forms of employee fraud that were highly prevalent in the bank include; forgery of customer's signature with a mean rating of 1.57 and computer

frauds (2.15). Other forms of employee fraud present to at a lower prevalence than the above include: opening and management of fictitious accounts (2.24) These findings imply that the most prevalent forms of employee fraud were cash theft, forgery of customer's signature and computer frauds.

**Table 4.4: Employee Fraud**

Employee Fraud Variables	N	Minimum	Maximum	Mean	Std. Deviation
Cash theft	30	1	3	1.53	.629
Forgery of customers signature	30	1	3	1.60	.675
Use of forged cheques to withdrawal monies	30	1	3	1.97	.765
Opening and operating fictitious accounts	30	1	2	1.47	.507
Diversion of funds e.g. to suspense accounts	30	1	2	1.37	.490
Valid N (listwise)	30				

**Source:** Research Data, 2019

#### 4.6 Forms of Third-Party Fraud

**Table 4.5: Third Party Fraud**

Third Party Fraud variables	N	Minimum	Maximum	Mean	Std. Deviation
Diversion of funds e.g. to suspense accounts	30	1	2	1.37	.490
Cheque fraud	30	2	4	3.40	.675
Misrepresentation and impersonation	30	2	4	2.93	.640
Computer/money transfer frauds	30	2	4	3.07	.740
Card Fraud	30	3	4	3.70	.466
Valid N (listwise)	30				

**Source:** Research Data, 2019



This study has identified the presence of employees and customer's fraud, employees and management fraud and employees and third-party frauds though at differing intervals and prevalence. All this can be categorized into third party frauds as they involve a third party. Forms of third-party fraud identified in this study in their descending order of prevalence were:

#### **4.7 Prevention and Control of Fraud**

This section presents the findings of the study on the most effective strategies for prevention and control of fraud.

##### **4.7.1 Strengthening of the Internal Control**

According to 60.00% of the respondents to this study, strengthening of internal controls and the accounting systems was a very effective strategy towards prevention and control of fraud. In addition, 33.33% of the respondents indicated that strengthening of internal controls was an effective strategy towards prevention and control of fraud. And the last 2 groups of responders who assume strengthening of internal control and accounting systems is less effective and have no effect are 3.33% each. This indicates that PBZ ltd should focus their strategy to implement better and modern scheme of control accounting systems in order to prevent fraud cases.

**Table 4.6: Strengthening of Internal Control**

<b>Variable</b>	<b>Very Effective</b>	<b>Effective</b>	<b>Least Effective</b>	<b>No effect</b>
Strengthening of the internal control and accounting systems	60.0 %	33.3%	3.33 %	3.33%

**Source:** Research Data, 2019

#### 4.7.2 Assessment and Prosecution of Fraud Cases

Out of all the respondents who answers the questionnaires, 33.3% of the respondents indicated that assessment and prosecution of fraud cases was the most effective strategy towards control of fraud. Forty-five-point six (45.6) percent indicated that was effective while 21.08 % indicated that it was least effective. This shows that to most respondentø prosecution of fraud cases was effective in prevention and control of fraud, this will be a good time for PBZ ltd to analyse its legal strategy to mitigate the fraud cases in the bank.

**Table 4.7: Assessment and Prosecution of Fraud Cases**

Variable	Very Effective	Effective	Least Effective	No effect
Assessment and prosecution of fraud cases	33.3 %	45.62 %	21.08 %	0.0 %

**Source:** Research Data, 2019

#### 4.7.3 Higher Remuneration for Employees

Higher remuneration for employees was an effective strategy for prevention and control of fraud. This is according to 73.33% of the respondents who indicated that it was most effective and the remainder which is 26.67% indicated that it was effective. As seen in table 4.8, responders who saw increasing remuneration of employees is least effective or no effect at all is 0%, this shows that once you pay your staff well, it will lead to less fraud in the bank. The PBZ management should consider this strategy since banking sectors are paying their workers good amount of money in order to reduce fraud cases in the bank.

**Table 4.8: Higher Numeration of Employees**

Variable	Very Effective	Effective	Least Effective	No effect
Higher numeration of employees	73.3 %	26.67 %	0 %	0 %

**Source:** Research Data, 2019

#### 4.7.4 Having Policies to Track Employees Conduct and Background

Implementation of policies to track employees conduct and background is a very effective strategy towards prevention and control of fraud. 33.3 % of the respondents indicated that it was effective to have policies that can track employees while 40.0 % indicated that it was effective strategy while 26.67% indicated that it was least effective to track employees background and conduct from where they are coming from.

**Table 4.9: Having Policies to Track Employees Conduct**

Variable	Very Effective	Effective	Least Effective	No effect
Having policies to track employees conduct and background	33.3 %	40.0 %	26.7 %	0.0 %

**Source:** Research Data, 2019

#### 4.7.5 Establishing fraud Reporting Centres and Hotlines

Furthermore, this study found that the use of fraud reporting centres and hotlines was effective in controlling and preventing fraud. 33.3% of the respondents indicated that it was most effective, 40.0% indicated that it was effective and 26.7% indicated that it was not effective. The hotlines usually help the bank to receive instant information from the customers and this enable them to be able to fight the fraud cases easily.

**Table 4.10: Establishing Fraud Reporting Centers and Hotlines**

Establishing fraud reporting centres and hotlines variable		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Least Effective	8	26.7	26.7	26.7
	Effective	12	40.0	40.0	66.7
	Very Effective	10	33.3	33.3	100.0
	Total	30	100.0	100.0	

**Source:** Research Data, 2019

#### 4.7.6 Ensuring shuffling and Mandatory Vacations for Employees

Shuffling and mandatory vacations for employees was an effective strategy for the control and prevention of fraud. This is according to 50.0% of the respondents. 33.3% of the respondents indicated that shuffling and mandatory vacations for employees was the most effective strategy while 16.7 % of the respondents indicated that it was the least effective strategy. People or workers who stay at the same work area for very long, it enables them to know the weak links and its mandatory to shuffle them whenever necessary, but they should be sure it won't affect the performance of the PBZ ltd.

**Table 4.11: Ensuring shuffling and Mandatory Vacations for Employees**

Ensuring shuffling and mandatory vacations for employees variable		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Least Effective	5	16.7	16.7	16.7
	Effective	15	50.0	50.0	66.7
	Very Effective	10	33.3	33.3	100.0
	Total	30	100.0	100.0	

**Source:** Research Data, 2019

#### **4.7.7 Other Strategies**

Respondents indicated other strategies that could be used to prevent and control fraud in the Bank. Some of the strategies identified include: upgrading the ATM cards used from magnetic strips to chip and enhancing pins, educating customers on card safety, proper procurement and disposal systems, open door policies for employees, staff training and treatment of fraud cases by employees equally. All these strategies are very important to make sure the prevention of the fraud cases is reduced; the workers promise to work and use the mentioned strategy to benefit the bank and increase performance in PBZ ltd.

#### **4.8 Discussion of the Findings**

The study used majority of its respondents from fraud auditors and supervisors who had the primary responsibility of detecting and preventing fraud. This enhances the findings of the study. The study found that fraud in PBZ ltd was accorded very high priority. The major causes of fraud in the bank were availability of opportunities for fraud, rationalization of fraud acts and pressure to commit fraud. This study found that there are very effective strategies to prevent and control fraud. However, the most effective strategies for prevention and control of fraud are: strengthening of internal controls and systems, performance management, improvement and hiring systems and policies, use of expected and unexpected audits and use of analytical tools.

These results resemble the research done by Yazdanifard, et al. (2011) whom explain that since the introduction of online banking, there have been rapid increases in its growth until 2004 when the first case of online fraud was reported, which is now

causing a decline in the nature of online banking. The criminals uses different methods or software such as Fishing; accessing into customers account by sending them fake e-mails telling them to submit their personal information. The online banking business has suffered great decline because of these flatulent activities.

These attacks have also affected customer trust to online banks and their confidence that the banks are unable to protect their assets and money which now lead banks to spend extra money seeking for solution in other to gain back their customers trust. The numbers of fraudulent activities committed identified by RSA was 18079 worldwide with 11 per cent increase from January 2011. Several banks and institution has come up with new approach in developing customer trust which includes enhancing communication and transparency about banks fraud and security, refund arrangement effectiveness on trust and introducing layered security strategy as well as analyzing solution that delivers customers trust and comfortability. In order to achieve this the banks were able to introduce some security measures that are able to reduce fraudulent activities like the implementation of KeCRIPT- not possible to fake, forge or fooled tested and proved 100 per cent protection, multifactor authentication that challenge suspected transaction by asking the user for additional questions.

The use of spyware software to protect computers against Trojan virus and removing them from infected computers as well. All of the discussion and the improvements are to encourage people to bank online and to increase security against fraud criminals as well as customers trust. Another study which resemble the result

obtained from this research including the research done by (Jamaliah ,2017) which shows that the study attempts to integrate ethical values into the fraud triangle theory in the context of Malaysian banking industry. Primary data were collected through the survey of 108 questionnaires administered to the employees of the top three largest banks in Malaysia.

The findings revealed that ethical values were negatively related to employee fraud, and two elements of fraud triangle theory, namely, opportunity and rationalization, were positively related to employee fraud. This implies that high ethical value is crucial to mitigate employee fraud. To minimize employee fraud, the banking industry should reduce opportunities and employee negative rationalization through strong internal control. This study contributes to literature on the occurrences of employee fraud, which is not widely discussed, especially in the context of the banking industry in developing countries.

In both research it shows that improving internal controls and systems will give good results in combatting the fraud cases in banks. Adding to that the results differ from the study done by Said et al (2017) on Integrating ethical values into fraud triangle theory in assessing employee fraud: Evidence from the Malaysian banking industry, the study found a negative relationship between ethical values and employee fraud occurrence, thereby supporting the fourth hypothesis. Hence, high ethical values among employees result in few employee fraud occurrences. Employees tend to comply with ethical behaviour during operations and services. Following ethical standards increases the belief among employees that ethical practice does not depend on situation, and thus, organization should enhance its standard code of ethics.

Haron et al. (2011) agreed that the function of ethical values as influential factor can lead to fraudulent behaviour among employees. Ethical values embraced individually can influence employees to abide by the organizational policies set by the management and avoid breach of rules among employees.

These findings are similar to the findings of Kingsley (2012) in his study on banking fraud in Nigeria. In the study, Kingsley (2012), found that institutional factors that lead to fraud may include but are not limited to weak accounting system control systems, inadequate supervision of subordinates, poor information technology and data base management, hapless personnel policies, poor salaries and general frustration occasioned by management unfulfilled promises. Other factors identified by Kingsley (2012), ACFE (2009), include, failure to engage in regular call over, employees refusal to abide with laid down procedures without any penalty, banks reluctant to report fraud due to the perceived negative publicity, banking experience of staff and inadequate infrastructure that may include poor communication systems result to a build-up of unbalanced posting, inadequate training, poor book keeping and genetic traits like kleptomaniac who pathologically steals for fund.



## **CHAPTER FIVE**

### **CONCLUSIONS & RECOMMENDATIONS**

#### **5.1 Introduction**

Chapter five discusses the findings and results presented in Chapter four. Discussion is in view of the findings of this study and those of other scholars and researchers. In addition, this chapter presents conclusions and recommendations for the study.

#### **5.2 Summary of the Main Findings**

This study sought to assess fraud in the banking industry in Tanzania using People bank of Zanzibar limited as the case. The objectives of the study were: To identify types of factors of electronic fraud in PBZ bank, to assess effects of factors influencing electronic fraud in PBZ bank, to establish relationship between factors influencing electronic fraud and their impacts to the PBZ bank and to develop a framework of deterrence, prevention, detection and remedies in terms of countermeasures against electronic fraud in PBZ bank.

The study utilized a descriptive research design using PBZ ltd bank as the case study. The research was conducted using PBZ ltd workers whom are 30 respondents in which they are working day to day in the bank and are all aware of the fraud cases in the banks, the author wanted to use different department found in the bank including, accounting section, risk section, ICT department and others to mention few. Data for the study was collected using a questionnaire given to workers which will be seen in appendix of this study. The data collected was analysed using SPSS vs. 20 for means, frequency distributions, standard deviations and modes. Analysed data was presented using figures and tables for ease of interpretation and elaboration.

The study found that fraud in PBZ limited was accorded very high priority issue. The major reasons of fraud in the bank were accessibility of opportunities for fraud, rationalization of fraud acts and pressure to commit fraud. Prospects for fraud were present due to comfortable internal controls and accounting systems, inadequate supervision of subordinates, disregard for customer due diligence requirements and poor personnel policies.

This study found that there are very current strategies to stop and control fraud. However, the most effective strategies for prevention and control of fraud are: use of ICT tools such as passwords and firewalls, strengthening of internal controls and systems, and recognition of employees, improvement and hiring systems and policies, use of expected and unexpected audits etc. All these strategies to combat fraud are very important for banks to analyse where they are now and where are they going to be in future, it's very important PBZ limited to start upgrading their banks systems and policies in order to meet international standards.

The customers also in Zanzibar and other part of Tanzania may have to ensure that their debit cards and other confidential passwords are kept safe and secured, and to report any loss or suspicion. The knowledge of how customers can interact quickly with the bank is very important in fighting the fraud issues. One of the bank Manager said to the author that electronic fraud occurs most of the time because of users' mistakes that needed to be addressed. This again implies a re-orientation of the customers in being security conscious as a requirement of the new system. The existing sociocultural norms, which influence customers' orientation, may have to be adapted.

Adding to that, the involvement and active participation of the staff and the organisational culture is also vital to the success of the technological measures used in fraud detection. Staff training in PBZ bank is vital and should be among new requirements of the procedural change and technological measures may have to become regular to establish a new culture in the bank. This would provide staff with the necessary skills, exposure and experience to address the issues that lack of skills and confidence of staff has contributed to the experience of electronic fraud. This implies changes in the organisational practices of the banks to reflect and adapt to the demands of technological changes.

### **5.3 Implications of the Findings**

The findings suggest that, in spite of the increase in the rate of online fraud, the rate of prosecution for online fraud offenders is very low. This implies low or lack of remedy activities on the part of the banks and other regulating authorities, as noted by some participants. The implication of this passivity is that it makes people believe that online fraud is not a crime, or that there has never been any online fraud. Thus, it encourages, rather than discourages, the continuation of the wrongful acts of online fraud.

Furthermore, fraudsters need to hide and clear their tracks; therefore, bank staff use advanced technologies, and other prosecuting / investigating officers need to be skilled and trained in technology. The findings show that this required skill and training is lacking and has affected the giving of punishment or reward for any fraudulent act. The implication is that the preparedness of officers is based on and may be guaranteed by the provision of training and an adequate infrastructural base.

## **5.4 Conclusion**

This chapter has presented the findings and results of the study. The study used majority of its respondents from fraud auditors and supervisors who had the primary responsibility of detecting and preventing fraud. This enhances the findings of the study. The study found that fraud in PBZ Ltd was accorded very high priority. The major causes of fraud in the bank were availability of opportunities for fraud, rationalization of fraud acts and pressure to commit fraud. This study found that there are very effective strategies to prevent and control fraud. However, the most effective strategies for prevention and control of fraud are: strengthening of internal controls and systems, performance management, improvement and hiring systems and policies, use of expected and unexpected audits and use of analytical tools.

## **5.5 Recommendations**

These recommendations are for policy making at the organization/ industry level. Furthermore, these recommendations can be utilized at the practice or management level.

### **5.5.1 Recommendations to the Bank**

Management of PBZ Ltd bank is generally advised to look way forward to address issues of non-management staff committing frauds by higher percentage compared to other groups outsiders and management staff by surveying and restructuring salaries/ remuneration to matching with responsibilities, inflation rate and profit banks are making. Management of banks should ensure fraud audits which are planned and unplanned are conducted to ensure elements of frauds or gaps in controls are early identified before resulting to loss to the banks. By doing so it will

be easy to prevent the problem before it occurs

In order to ensure fully accountability for making decision to deter frauds in banks, management of banks are advised to set fraud threshold on which either single incident of fraud or cumulative beyond the set limit the top management would be accountable irrespective of who caused the fraud. This will create proactive prevention of frauds to avoid accountability. Awareness to the bank is very important to combat fraud, management of banks further is advised to ensure there is programme for public awareness on common frauds such of card frauds which appeared to be a result of customer knowledge on protecting their cards and password.

### **5.5.2 Recommendations to the Bank Regulator**

The bank regulator in Tanzania is advised to set threshold for losses resulted from frauds as either single incident or cumulative in a year and beyond, leads bank top management being held accountable irrespective of who cause the loss/fraud. Moreover, the bank regulator is advised to initiate measures of establishment of specific court to deal with frauds resulted from commercial banks where it will assist to recover the fraudulent funds timely rather than focusing on sentencing the convicted whereas the loss steal stands in banks. The legal framework should be reviewed to make sure the penalties are going with today's world in order to eradicate this problem.

### **5.6 Research Limitations**

Due to the shortage of time and resources, the author faced the lack of data due to

the Zanzibar (Tanzania) environmental conditions inside the Banks and that has led to affect some parts of project analysis. There was lack of documented data in some areas which enforced the researcher to mostly rely on external publications to support the study. The study also did not cover technical part of the previous cases and details of the banking transactions which is being used in the banks procedures in order to maintain the ethical conditions of accounts confidentiality of the banks.

The study focused on the factors influencing electronic fraud in banking industry in Tanzania with PBZ as a case study and how these factors can be effectively controlled in PBZ bank ltd. The study is therefore limited to the countermeasures designed and deployed by PBZ bank Ltd to fight electronic fraud. The technical and economic feasibility of the countermeasures were not the focus of this study and therefore were not fully examined. The study is also limited to specific electronic fraud related to E-banking and E-commerce transactions. Other types of E-fraud such as online auction fraud and other cybercrimes were not examined in the domain of the study.

### **5.7 Recommendations for Further Studies**

To validate the findings of this study, this study recommends that future studies be replicated in different banks or financial institutions. This could be undertaken in a large bank especially the top 5 banks in asset size in Tanzania or the East African region. Furthermore, a similar study using multiple banks could also provide substantive literature for comparison. This could provide literature for comparison to the findings of this study.

Adding to that, other researchers are recommended to conduct study to establish why managements sometimes do not implement full the auditor's recommendations. The author senses the need of more works in future to be done on analysing certain decision making in the bank and their implications to the day to day operations of the bank and how those decisions are affecting fraud preventions. This weakness if left unattended may expose the banks to financial losses which would have been prevented.

## REFERENCE

- Abiola, I. (2015). Internal Control System on Fraud Detection: Nigeria Experience. Ladoke Akintola University of Technology, Nigeria.
- ACFE, (2018). Discussion on the Fraud Triangle, Association of Certified Fraud Examiners, ACFE.
- Adeleye, B. C., Annasingh, F., & Nunes, M. B. (2004). Risk management practices in IS outsourcing: an investigation into commercial banks in Nigeria. *International Journal of Information Management*, 24, 167-180.
- Adeyemi, S. B. & Okpala, O. P. (2016). The Impact of Audit Independence on financial Reporting: Evidence from Nigeria. Nigeria.
- Afayi, T. (2014). *The effect of fraud on the performance of banks in the United States of America*. Plainview: Wayland Baptist University.
- Akelola, S. (2014). *Fraud in the banking industry: a case study of Kenya*. Published PhD. Thesis, Nottingham: Nottingham Trent University.
- Akinyomi, O. J. (2012). Examination of fraud in the Nigerian banking sector and its prevention. *Asian Journal of Management Research*, 3(1), 184-192.
- Ampratwum, E. F. (2009). Advance fee fraud and investor confidence in the economies of sub-Saharan African (SSA). *Journal of Financial Crime*, 16 (1), 67-79.
- Anyango (2018). *Effects of Leadership styles on Employee Performance at BOA Kenya limited*. Unpublished masters dissertation, Open University of Tanzania, Dar es Salaam, Tanzania.
- Barker, S. E. & Edwards, R. (2012). How many qualitative interviews is enough? Expert contribution in how many qualitative interviews is enough? National



Centre for Research Methods Review Paper, NCRM.

Bhasin, M. (2016). Frauds in the Banking Sector: Experience of a Developing Country. *Asian Journal of Social Sciences and Management Studies*, 3, 1-9.

BOT, (2018). *Deposit Insurance Bank of Tanzania, Publications and Statistics*, Dar es Salaam: BOT.

Bryman, A. (2001). *Social Research Methods*. Oxford: Oxford University Press.

Chartered Institute of Management Accountants (CIMA), (2009). *Fraud Risk Management: A Guide to Good Practice*, a guide to good practice, CIMA.

Chiemeke, K. C., Choi, S. L. & Haprizu, B. T. (2012). *The Relationship Among Job Satisfaction, Organizational Commitment and Employees' Turnover at Unilever Corporation in Nigeria*. *European Journal of Multidisciplinary Studies*.

Chimwemwe, C. & Muthinja, M. (2018). Financial innovations and bank performance in Kenya: Evidence from branchless banking models. *South African Journal of Economic and Management Sciences*, 21(1), 1-11.

Collins, S. & Carpenter, R. & Orenstein, D. & Whitmer, A.C. (2011). An Integrated Conceptual Framework for Social Ecological Research. *Frontiers in Ecology and the Environment*. 9, 351-357.

Creswell, J. W. (2008). *Educational research: planning, conducting, and evaluating quantitative and qualitative research*, 4<sup>th</sup> Ed., London: Pearson.

Dawson, C. (2018). *Research Methodology, Methods and Techniques*, Oxford: Oxford University Press.

DiCicco-Bloom, B. (2018). *Why use computers in qualitative research?* Carfonia: Blackwell Publishing Ltd.

- Dorgham & Al-Halabi, (2014). The Impact of Management Control Systems on Limiting Fraudulent Practices in Manufacturing Companies. *Research Journal of Finance and Accounting*, 3(1), 1-14.
- Evans, J., & Dadzie, K. (1998). Corporate governance and the fragility of banking systems in developing countries: An analysis of a credit market in Ghana. *Global Finance Journal*, 9(1), 109-125.
- Ganesh, A. & Raghurama, A. (2008). Status of training evaluation in commercial bank- a case study. *Journal of Social Sciences and Management Sciences*, 37(2), 137-158.
- Gary, P. (2018). Customer Liability in the Age of Digital Banking, digital demand report, Oracle Financial Services Global Retail Banking Survey, ORACLE.
- Geffner, M. (2018). How Banks Fight Electronic Banking Fraud, Bankrate, research paper No. 2017/007.
- Goswami, S. (2017). Mobile Banking ó The Future. Hyderabad Technologies. *Journal of Internet Banking and Commerce*, 22(8), 1-13.
- Hanibal, G. (2018). Jurisdictions East African Community, Global Legal Monitor. Archive for Jurisdiction: Kenya.
- Haron, H., Ismail, I., & Abdul Razak, S. H. (2011). Factors Influencing Unethical Behavior of Insurance Agents. *International Journal of Business and Social Science*, 2(1), 1-17.
- Hillison, W. & Pacini, C. & Sinason, D. (1999). The internal auditor as fraud-buster. *Managerial Auditing Journal*, 14. 351-363.
- Hoffmann, A. O. (2012). The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking. *International*

*Journal of Bank Marketing*, 30(5), 390-407.

- Kalimangasi, N., Bundala, D. M. and Mlowosa, T.P. (2014). Measuring Contributions of Information Technology on Bank's Service Offering: The Case of National Microfinance Bank (NMB) Ltd Tanzania. *International Journal of Scientific and Research Publications*, 4(11), 2250-3153.
- Kieran, J. (2018). An Overview of Research on Auditor's Responsibility to Detect Fraud on Financial Statements, Taiwan.
- Kothari, C. R. (2004), *Research Methodology: Methods and Techniques*, (Second Edition), New York: New Age International Publishers
- Lab, K. (2018). *Introducing Kaspersky Fraud Prevention*, KASPERSKY.
- Leonard, A. (2013). An Assessment of Fraud and its Management in Tanzania Commercial Banks: The Case of CRDB and NMB Banks Plc. Tanzania. Unpublished masters dissertation, Mzumbe University, Morogoro, Tanzania.
- Masamila, Bossi. (2014). State of Mobile Banking in Tanzania and Security Issues. *International Journal of Network Security & Its Applications*. 6, 53-64.
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*, (2<sup>nd</sup> ed.), Thousand Oaks, CA: Sage.
- Mohottige, G., Sujeewa, M., Shukri, M., Yajid, A. Khatibi, S. M., & Dharmaratne, F. A. (2017). Integrating ethical values into fraud triangle theory in assessing employee fraud: Evidence from the Malaysian banking industry. *Journal of International Studies*, 10(2), 170-184.
- Noralina. (2015). Fraud Detection and Prevention Methods in the Malaysian Public Sector: Accountants' and Internal Auditors' Perceptions. *Procedia Economics and Finance*. 28(1), 59-67.

- Odi, N. (2013). Implication of fraud on commercial banks performance in Nigeria, *International Journal of Business and Management*, 8(15), 144-150.
- Ojeaga, P. (2018). Do High Customer Bank Deposits Incite Management Fraud? Examining Causes of Management Fraud in the Nigerian Banking Sector. *Journal of Educational and Social Research*, 4(6), 1-2.
- Olaniyan, T. (2018). The Impact of Fraud on the Performance of Deposit Money Banks in Nigeria. *International Journal of Innovative Finance and Economics Research*, 6(1), 40-49.
- Onkagba, J.O. (1993). *Auditing Computerization Information System: A Growing Audit Challenge*. The Nigerian Accountant, Lagos, Published by ICA|N, Jan/Mar.
- Pal, S. (2016). A review on customer satisfaction with internet banking in public and private bank. *International Journal of Engineering Sciences & Research Technology*, 6(3), 261-274.
- Pan, G. (2011). Fraud: A Review and Research Agenda. *Accountancy Business and the Public Interest*. 10, 138-178.
- Peng & Turban (2009) *Electronic Commerce: A Managerial Perspective*. New Jersey: Pearson Education.
- PWC, (2011). *Fighting fraud in the public sector*, Kuala Lumpur. Retrieved on 20<sup>th</sup> March, 2018 from; [whatwouldyouliketogrow.com.au](http://whatwouldyouliketogrow.com.au).
- Rahman, R. & Syahira, K. & Irda, A. (2014). Effectiveness of Fraud Prevention and Detection Techniques in Malaysian Islamic Banks. Malaysia. *Procedia - Social and Behavioral Sciences*, 145, 97 ó 102.

- Said, J., Alam, M. M., & Rafidi, A. (2017). *Integrating ethical values into fraud triangle theory in assessing employee fraud: Evidence from the Malaysian banking industry*. *Journal of International Studies*, 10(2), 170-184.
- Samuel, O. (2018). Fraud in Nigerian Banks. *Journal Fin. Mark*, 2(3), 14-22.
- Shewangu, D. (2018). Financial consumer protection: internet banking fraud awareness by the banking sector. *Article Info*, 11(4), 127-134.
- Soral, H, Talan & Hebb, Gregory. (2006). Fraud, banking crisis, and regulatory enforcement: Evidence from micro-level transactions data. *European Journal of Law and Economics*, 21. 179-197.
- Tawa, J. (2018). *A method for collecting and interpreting interpersonal behavioural data in Second Life: A sample study on Asians', Blacks', and Whites' social distances*.
- Tero, P. & Carry, P. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model, *Internet Research*, 14(3), 224-235.
- The Balance, (2018). Learn About Being Protected from Electronic Banking Fraud and Errors, overdraft notes, The Balance.
- Udeh, S. N., & Ugwu, J. I. (2018). *Fraud in Nigerian Banking Sector*. *International Journal of Academic Research in Business and Social Sciences*, 8(5), 589-607.
- Walton, L., Brown, D., Rahman, M. & Nuri, R. (2012). Reliability and Validity of Bengali Language SF-36 and IIG-7 for Utilization in Postpartum Bangladeshi Women.
- Wekesa, M. M., Simiyu, G., Namusonge, N. (2016). Determinants of Effective Fraud Management: A Survey of Domestic Tier One Commercial Banks in

Trans Nzoia County, Kenya. *International Journal of Scientific and Research Publications*, 6(10), 12-18.

Yazdanifard, W. & Behora, C. & Sade, A. (2011). Electronic banking fraud; the need to enhance security and customer trust in online banking. *International Journal in Advances in Information Sciences and Service Sciences*. 3, 505-509.

Yin, R. K., (1994). *Case Study Research Design and Methods: Applied Social Research and Methods Series*. CA: Sage Publications Inc.

## APPENDIX

### QUESTIONNAIRE ON FACTORS INFLUENCING ELECTRONIC FRAUD IN THE BANKING INDUSTRY IN ZANZIBAR, TANZANIA

**Introduction:** Dear Respondent, my name is Haji Maulid and I am a student at Open University currently pursuing Masters of Business Administration. Please, kindly fill in the questionnaire below that seeks your opinion regarding fraud issues related to The People's Bank of Zanzibar (PBZ) Limited. The information provided will solely be consumed for academic research purposes and your identity and opinions will remain confidential. Any information provided will be treated with utmost confidentiality and no single responses will be reported on its own, but as a summation of all the responses. Participation is entirely voluntary. There is no foreseeable harm in taking part in this study and you can choose to withdraw from participating at any point. Your response will be kept strictly confidential and data reported anonymously. Should you have any queries or need clarification on this regard, please feel free to contact me at 0777 451138 I thank you well in advance for your time.

#### PART 1: DEMOGRAPHIC INFORMATION

**Please Tick the Answer to Your Question**

1. What is Your Gender?	Male		Female	
2. Which age group do you belong to?	18 - 30	31-50	51-60	Above 60
3. What is your education level?	Certificate	Diploma	Degree	Postgraduate
4. What is your role in the bank?	Senior Manager Assistant	Manager/ Supervisor	Auditor/ Risk Manager	Operations Assistant/Clerks
5. How long have you worked for the bank?	Less than 1 yr	1 to 5 yrs	5 to 10 yrs	Above 10 yrs

## PART 2: PERCEPTION OF FRAUD IN PBZ BANK LIMITED

Please choose by a tick (✓) the extent to which you agree with the following Fraud Management statements at PBZ

(1 = Strongly Disagree; 2 = Disagree; 3 = Neutral; 4 = Agree; 5 = Strongly Agree)

No.	PBZ Fraud Management	1	2	3	4	5
1	PBZ Ltd has been successful in fighting fraud in their bank					
2	PBZ Ltd is up to date with emerging fraud trends in the banking industry					
3	Fraud policy is well communicated in PBZ Ltd to all departments					
4	PBZ Ltd gives importance to fraud incidences in the bank at all times					

## PART 3: TYPES OF FRAUD

No.	Management Fraud	High	Average	Low	No Effect
5	Overstatement of assets				
6	Overstatement of revenues				
7	Understatement of liabilities				
8	Understatement of expenses				
9	Cash theft				
10	Forgery of customers signature				
11	Use of forged cheques to withdrawal monies				
12	Opening and operating fictitious accounts				
13	Diversions of funds e.g. to suspense accounts				
14	Cheque fraud				
15	Misrepresentation and impersonation				
16	Computer/money transfer frauds				
17	Card Fraud				



**PART 4: PREVENTION OF FRAUD**

<b>No</b>	<b>Preventing Fraud</b>	<b>Very Effective</b>	<b>Effective</b>	<b>Least Effective</b>	<b>No Effect</b>
18	Strengthening of the internal control and accounting systems				
19	Assessment and prosecution of fraud cases				
20	Higher remuneration for employees				
21	Having policies to track employees conduct and background				
22	Establishing fraud reporting centres and hotlines				
23	Ensuring shuffling and mandatory vacations for employees				